Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

ON THE CONGRUENCE $cx^\lambda + 1 \equiv dy^\lambda$ IN A GALOIS FIELD.*

BY HOWARD H. MITCHELL.

Introduction.

1. In another paper† the author has considered the relation between a certain cyclotomic function and the congruences

$$cx^\lambda + 1 \equiv dy^\lambda$$

in a Galois field of order q^t, where $q^t = \lambda\nu + 1$, and c, d are any marks in the field different from 0. If c and d are expressed as powers of a primitive root in the field, and

$$\text{ind } c \equiv i, \qquad \text{ind } d \equiv j, \qquad \text{mod } \lambda,$$

we shall denote the number of solutions of the congruence by m_i^j. The object of the present paper is to obtain certain results concerning the numbers m_i^j.

For the case where q is a prime of the form $\lambda\nu + 1$ and $t = 1$ the problem has been considered by a number of other authors. Gauss showed that for $\lambda = 3$ the determination of the numbers m_i^j could be accomplished by means of the representation of $4q$ by the form $A^2 + 27B^2$, and for $\lambda = 4$ by means of the representation of q by the form $A^2 + B^2$. In a recent paper Dickson obtained a lower limit for the number of solutions when λ is prime and $c \equiv d \equiv 1$, mod q, and thereby showed that solutions exist for every q exceeding a certain limit in terms of λ. Hurwitz later extended this result by obtaining both upper and lower limits for any pair of residues c, d.‡

The author obtains three results in the present paper. By means of certain properties of congruences it is first shown that the values of the numbers m_i^j are completely determined by means of a particular set of equations. By means of this result the exact values of these numbers are found for a Galois field of order q^{2t}, provided t has a divisor t_1 such that $q^{t_1} \equiv -1$, mod λ. Finally it is shown that, if $q^t \equiv 1$, mod λ, the numbers

---

* Presented to the American Mathematical Society, Dec. 28, 1915.

† Transactions of the American Mathematical Society, vol. 17 (1916), pp. 165–177.

‡ Gauss, Disquisitiones Arithmeticæ, § 358; Theoria Residuorum Biquadraticorum, §§ 15–20; Lebesgue, Journal de Mathematiques, vol. 2 (1837), pp. 253–292; Carey, Quarterly Journal of Mathematics, vol. 26 (1893), pp. 322–371; Dickson, Journal für Mathematik, vol. 135 (1909), pp. 181–188; Hurwitz, ibid., vol. 136 (1909), pp. 272–292; Cornacchia, Giornale di mathematische di Battaglini, vol. 47 (1909), pp. 219–268.

m_i^j for a field of order q^{st} may be expressed in terms of the similar numbers for a field of order q^t.

A lemma concerning congruences.

2. In what follows we shall denote by the symbol $dv(a, b, c, \cdots)$ the greatest common divisor of the integers $a, b, c, \cdots$. We consider a, b to be any pair of residues, mod λ, such that $dv(\lambda, a, b) = 1$. We shall also regard ka, kb as the same as a, b provided k is prime to λ. The total number of such pairs is equal to

$$\frac{\varphi_2(\lambda)}{\varphi(\lambda)},$$

where

$$\varphi(\lambda) = \lambda\Pi\left(1 - \frac{1}{\pi_i}\right), \qquad \varphi_2(\lambda) = \lambda^2\Pi\left(1 - \frac{1}{\pi_i^2}\right)$$

are the φ-functions of the first and second order respectively,* and where the products are to be taken over the different primes π_i contained in λ.

We shall need to determine for how many such pairs a, b

$$dv(\lambda, ax + by) = \frac{\lambda}{\tau}, \tag{1}$$

where x, y are any integers, and τ is a divisor of λ. If we write

$$dv(\lambda, x, y) = \sigma, \tag{2}$$

it is evident that there will be no such pairs if λ/τ is not divisible by σ.

We shall prove

Lemma 1. *The number of pairs of residues a, b, mod λ, such that*

(*a*) $dv(\lambda, a, b) = 1$,

(*b*) *ka, kb is regarded as the same as a, b if k is prime to λ,*

(*c*) *condition* (1) *is satisfied,*

(*d*) *λ/τ is divisible by σ, is equal to*

$$\sigma\Pi\left(1 + \frac{1}{\pi_i}\right) \times \tau\Pi\left(1 - \frac{1}{\pi_j}\right),$$

where the first product is to be taken over all the different primes π_i that are contained in σ to as high a power as in λ, and the second product over all the different primes π_j that are contained in τ, but not to as high a power as in λ/σ.

We put

$$dv\left(\frac{\lambda}{\tau}, x\right) = \beta\sigma, \qquad dv\left(\frac{\lambda}{\tau}, y\right) = \alpha\sigma,$$

so that α and β have no common factor, and write also

$$\lambda = \alpha\beta\rho\sigma\tau.$$

---

* Cahen, Elements de la Theorie des Nombres, 1900, p. 36.

In order that

$$ax + by \equiv 0, \qquad \text{mod}\,\frac{\lambda}{\tau},$$

a must be divisible by α, and b by β, so that we have

$$\frac{a}{\alpha}x' + \frac{b}{\beta}y' \equiv 0, \qquad \text{mod}\ \rho, \tag{3}$$

where $x' = x/\beta\sigma$, and $y' = y/\alpha\sigma$, are each prime to ρ.

In order that $dv(\rho,\ a,\ b) = 1$, a/α and b/β must each be prime to ρ, and for each value of a/α, prime to ρ, there will be exactly one value of b/β, mod ρ, for which the congruence is satisfied. We shall at first consider ka, kb as different from a, b for $k \not\equiv 1$, mod λ, and hence we may consider the pairs a, b for which the congruence (3) is satisfied, and for which $dv(\rho,\ a,\ b) = 1$, to be divided into $\varphi(\rho)$ sets according to the residues of a/α, b/β, mod ρ.

The pairs a, b for which a/α, b/β have particular residues, mod ρ, may be represented by the equations

$$\frac{a}{\alpha} = \frac{a_0}{\alpha} + h\rho, \qquad \frac{b}{\beta} = \frac{b_0}{\beta} + l\rho,$$

where a_0, b_0 represent a particular pair such that a_0/α, b_0/β are each less than ρ, and $h = 0, 1, 2, \cdots, \beta\sigma\tau - 1$; $l = 0, 1, 2, \cdots, \alpha\sigma\tau - 1$.

In order that $dv(\alpha\beta,\ a,\ b) = 1$, we must choose h so that a is prime to β, and l so that b is prime to α. Since a/α is prime to ρ for all values of h, we merely need to choose h so that a/α is prime to $\bar{\beta}$, where $\bar{\beta}$ represents the product of all the factors contained in β that are prime to ρ. As h assumes the values of a complete residue system, mod $\bar{\beta}$, the same is true of $h\rho$, and hence also of a/α. There are consequently $\varphi(\bar{\beta})$ values of h, mod $\bar{\beta}$, and hence $\varphi(\bar{\beta})\beta/\bar{\beta}$ values of h, mod β, for which a/α is prime to $\bar{\beta}$.

Similarly, if $\bar{\alpha}$ represents the product of all the factors contained in α that are prime to ρ, there are $\varphi(\bar{\alpha})\alpha/\bar{\alpha}$ values of l, mod α, for which b/β is prime to $\bar{\alpha}$. Hence the pairs a, b for which the congruence (3) is satisfied, and such that $dv(\alpha\beta\rho,\ a,\ b) = 1$, may be divided into

$$\varphi(\rho) \cdot \varphi(\bar{\beta})\,\frac{\beta}{\bar{\beta}} \cdot \varphi(\bar{\alpha})\,\frac{\alpha}{\bar{\alpha}}$$

sets according to the residues of a/α, mod $\beta\rho$, and b/β, mod $\alpha\rho$.

The pairs a, b for which a/α has a particular residue, mod $\beta\rho$, and b/β a particular residue, mod $\alpha\rho$, may be represented by the equations

$$\frac{a}{\alpha} = \frac{a_1}{\alpha} + h'\beta\rho, \qquad \frac{b}{\beta} = \frac{b_1}{\beta} + l'\alpha\rho,$$

where a_1, b_1 represent a particular pair such that a_1/α and b_1/β are less than $\beta\rho$ and $\alpha\rho$ respectively, and h', $l' = 0, 1, 2, \cdots, \sigma\tau - 1$.

In order that condition (1) shall hold we must have

$$\text{(4)}\quad \frac{a}{\alpha}x' + \frac{b}{\beta}y' \equiv \left(\frac{a_1}{\alpha}x' + \frac{b_1}{\beta}y'\right) + (h'\beta x' + l'\alpha y')\rho \equiv \mu\rho, \qquad \text{mod } \tau\rho,$$

where μ is prime to τ. Since

$$\beta x' = \frac{x}{\sigma}, \qquad \alpha y' = \frac{y}{\sigma}, \qquad dv\left(\frac{\lambda}{\sigma}, \frac{x}{\sigma}, \frac{y}{\sigma}\right) = 1,$$

we have

$$dv(\tau, \beta x', \alpha y') = 1.$$

Hence by a proper choice of h', l', mod τ, we may make $h'\beta x' + l'\alpha y'$ assume any residue, mod τ. Moreover, there are exactly as many pairs h', l', mod τ, for which this expression assumes the residue 0, mod τ, as pairs for which it assumes any other residue, and hence the expression assumes any desired residue for exactly τ of the τ^2 pairs. Since there are $\varphi(\tau)$ residues μ, prime to τ, we conclude that there are $\varphi(\tau)\tau$ pairs h', l', mod τ, for which the condition (4) is satisfied.

Moreover, when condition (4) is satisfied, we have also $dv(\tau, a, b) = 1$. For all the pairs a, b that we are now considering satisfy the condition, $dv(\alpha\beta\rho, a, b) = 1$. Hence $dv(\tau, a, b)$ must be prime to $\alpha\beta\rho$. It then follows from condition (4) that it must have the value 1.

We conclude that the pairs a, b for which (4) is satisfied, and such that $dv(\alpha\beta\rho\tau, a, b) = 1$, may be divided into

$$\varphi(\rho) \cdot \varphi(\bar{\beta})\frac{\beta}{\bar{\beta}} \cdot \varphi(\bar{\alpha})\frac{\alpha}{\bar{\alpha}} \cdot \varphi(\tau)\tau$$

sets according to the residues of a/α, mod $\beta\rho\tau$, and b/β, mod $\alpha\rho\tau$.

The pairs a, b for which a/α has a particular residue, mod $\beta\rho\tau$, and b/β a particular residue, mod $\alpha\rho\tau$, may be represented by the equations

$$\frac{a}{\alpha} = \frac{a_2}{\alpha} + h''\beta\rho\tau, \qquad \frac{b}{\beta} = \frac{b_2}{\beta} + l''\alpha\rho\tau,$$

where a_2, b_2 represent a particular pair such that a_2/α and b_2/β are less than $\beta\rho\tau$ and $\alpha\rho\tau$ respectively, and where h'', $l'' = 0, 1, 2, \cdots, \sigma - 1$. For all these the condition (4) is satisfied, and $dv(\alpha\beta\rho\tau, a, b) = 1$. It remains only to impose the condition $dv(\sigma, a, b) = 1$. This will be true provided $dv(\bar{\sigma}, a, b) = 1$, where $\bar{\sigma}$ represents the product of all the factors contained in σ that are prime to $\alpha\beta\rho\tau$.

As h'', l'' assume independently the values of complete residue systems, mod $\bar{\sigma}$, the same is true of $h''\beta\rho\tau$ and $l''\alpha\rho\tau$, and hence also of a/α and

b/β. The number of pairs of residues, mod $\bar{\sigma}$, whose greatest common divisor is prime to $\bar{\sigma}$, is by definition $\varphi_2(\bar{\sigma})$.* Since there are $\sigma/\bar{\sigma}$ values of h'' for which a/α assumes a particular residue, mod $\bar{\sigma}$, and $\sigma/\bar{\sigma}$ values of l'' for which b/β assumes a particular residue, mod $\bar{\sigma}$, there are $\varphi_2(\bar{\sigma})\sigma^2/\bar{\sigma}^2$ pairs h'', l'' for which $dv(\bar{\sigma}, a, b) = 1$.

We conclude therefore that there are

$$\varphi(\rho) \cdot \varphi(\bar{\beta})\frac{\beta}{\bar{\beta}} \cdot \varphi(\bar{\alpha})\frac{\alpha}{\bar{\alpha}} \cdot \varphi(\tau)\tau \cdot \varphi_2(\bar{\sigma})\frac{\sigma^2}{\bar{\sigma}^2}$$

pairs a, b for which $dv(\lambda, a, b) = 1$, for which condition (4) is satisfied, and such that ka, kb is regarded as different from a, b if $k \equiv 1$, mod λ. Since we wish finally to regard such pairs as the same, we must divide the above number by $\varphi(\lambda)$. This may be written in the form

$$\varphi(\lambda) = \varphi(\rho) \cdot \varphi(\bar{\beta})\frac{\beta}{\bar{\beta}} \cdot \varphi(\bar{\alpha})\frac{\alpha}{\bar{\alpha}} \cdot \varphi(\bar{\tau})\frac{\tau}{\bar{\tau}} \cdot \varphi(\bar{\sigma})\frac{\sigma}{\bar{\sigma}},$$

where $\bar{\tau}$ represents the product of all the factors contained in τ that are prime to $\alpha\beta\rho$. Hence the desired result is

$$\bar{\tau}\frac{\varphi(\tau)}{\varphi(\bar{\tau})} \cdot \frac{\sigma}{\bar{\sigma}}\frac{\varphi_2(\bar{\sigma})}{\varphi(\bar{\sigma})}.$$

We may write

$$\varphi(\tau) = \tau\Pi\left(1 - \frac{1}{\pi_k}\right),$$

$$\varphi(\bar{\tau}) = \bar{\tau}\Pi\left(1 - \frac{1}{\bar{\pi}_k}\right),$$

$$\varphi_2(\bar{\sigma}) = \bar{\sigma}^2\Pi\left(1 - \frac{1}{\pi_i^2}\right),$$

$$\varphi(\bar{\sigma}) = \bar{\sigma}\Pi\left(1 - \frac{1}{\pi_i}\right),$$

where the first product is to be taken over all the different primes π_k contained in τ, the second over the different primes $\bar{\pi}_k$ contained in $\bar{\tau}$ (i. e., in τ, but not in $\alpha\beta\rho$), and the last two products over the different primes π_i contained in $\bar{\sigma}$ (i. e., in σ, but not in $\alpha\beta\rho\tau$). When we substitute these expressions in our result and make the possible cancellations, we obtain finally

$$\tau\Pi\left(1 - \frac{1}{\pi_j}\right) \times \sigma\Pi\left(1 + \frac{1}{\pi_i}\right),$$

where the first product is to be taken over all the different primes π_j contained in τ, but not to as high a power as in λ/σ, and the second over the different primes π_i contained in σ to as high a power as in λ. We have thus established Lemma 1.

---

* Cahen, l. c.

A system of equations which determine the numbers m_i^j.

3. We now consider the congruence

$$cx^\lambda + 1 \equiv dy^\lambda$$

in a Galois field of order $q^t = \lambda\nu + 1$ and denote the number of its solutions by m_i^j, where c and d are supposed expressed as powers of a primitive root in the field, and ind $c \equiv i$, ind $d \equiv j$, mod λ. Two solutions for which x^λ, y^λ have the same values will be considered as the same. The residue, ind (-1), mod λ, will be denoted by ϵ. This has the value 0 unless q and v are both odd, in which case it is $\lambda/2$.

The following relations between the numbers m_i^j are well known:

$$m_i^j = m_{j+\epsilon}^{i+\epsilon} = m_{-j+\epsilon}^{i-j} = m_{i-j+\epsilon}^{-j} = m_{-i}^{j-i} = m_{j-i+\epsilon}^{-i+\epsilon}; \tag{1}$$

$$\sum_i m_i^0 = \nu - 1; \qquad \sum_i m_i^j = \nu; \tag{2}$$

where $i = 0, 1, 2, \cdots, \lambda - 1$; $j \not\equiv 0$, mod λ.

Another relation may be easily proved. For from the given congruence we have

$$c^q x^{q\lambda} + 1 \equiv d^q y^{q\lambda}.$$

Conversely by raising this congruence to the power q^{t-1}, we conclude that if it is satisfied the given congruence must be. Hence we have $m_{qi}^{qj} = m_i^j$, or more generally

$$m_{i'}^{j'} = m_i^j, \tag{3}$$

provided for some integer k, $j' \equiv q^k j$, $i' \equiv q^k i$, mod λ.

We define $M_{a,b,c}$ to be sum of the λ numbers m_i^j for which the congruence

$$aj + bi \equiv c, \qquad \text{mod } \lambda, \tag{4}$$

is satisfied, where we suppose that $dv(\lambda, a, b) = 1$. The number of distinct congruences of this type is equal to

$$\frac{\varphi_2(\lambda)}{\varphi(\lambda)} \cdot \lambda = \psi(\lambda) \cdot \lambda.$$

Theorem 1. *The λ^2 quantities m_i^j are completely determined by the set of $\lambda\psi(\lambda)$ equations*

$$\Sigma m_i^j = M_{a,b,c}, \tag{5}$$

where the values of the numbers $M_{a,b,c}$ *are supposed known, and* i, j *assume as values the* λ *pairs of residues for which the congruence* (4) *is satisfied.*

We divide the equations (5) into sets with respect to a particular one of the numbers m_i^j, say $m_{i_0}^{j_0}$, as follows. We designate as an equation E_τ any one of the equations (5) for which

$$dv(\lambda,\, aj_0 + bi_0 - c) = \frac{\lambda}{\tau}. \tag{6}$$

Hence $m_{i_0}^{j_0}$ will appear in each of the $\psi(\lambda)$ equations E_1, and in none of the others.

We inquire how many times any other m_i^j will appear in the set E_τ. For any equation in this set we have

$$dv[\lambda,\, a(j - j_0) + b(i - i_0)] = \frac{\lambda}{\tau},$$

and hence if we put

$$\sigma = dv(\lambda,\, i - i_0,\, j - j_0), \tag{7}$$

it follows that λ/τ is divisible by σ.

By Lemma 1 the number of times m_i^j appears in the set E_τ is equal to

$$\sigma\Pi\left(1 + \frac{1}{\pi_i}\right) \times \tau\Pi\left(1 - \frac{1}{\pi_j}\right), \tag{8}$$

where the products are to be taken respectively over the different primes π_i contained in σ to as high a power as in λ, and the different primes π_j contained in τ, but not to as high a power as in λ/σ. We shall denote the second factor of the product (8) by $f(\tau)$, since in the discussion λ and σ will be supposed fixed.

We now multiply each of the equations E_τ by $(-1)^r/\chi(\tau)$, where $\chi(1) = 1$, whereas if

$$\tau = \pi_1^{e_1}\pi_2^{e_2}, \cdots \pi_r^{e_r},$$

$$\chi(\tau) = \pi_1^{2e_1-1}\pi_2^{2e_2-1} \cdots \pi_r^{2e_r-1}. \tag{9}$$

We then form the sum of all the equations thus obtained, τ being allowed to range over all the divisors of λ, and shall show that the result is

$$\psi(\lambda)m_{i_0}^{j_0} = \Sigma\frac{(-1)^r}{\chi(\tau)}M_{a,b,c}, \tag{10}$$

where the sum is taken over all the $\lambda\psi(\lambda)$ numbers $M_{a,b,c}$, and τ is defined by (6).

Since $m_{i_0}^{j_0}$ appears in each of the equations E_1, and in none of the others, the coefficient of $m_{i_0}^{j_0}$ in this sum is $\psi(\lambda)$. Another m_i^j cannot appear in any equations E_{τ} for which λ/τ is not divisible by σ, where σ is defined by (7). The coefficient of m_i^j in (10) is equal to the first factor of the product (8) multiplied by

$$(11) \qquad \Sigma(-1)^r \frac{f(\tau)}{\chi(\tau)},$$

where the sum is to be taken over all the divisors τ of λ/σ, and r denotes the number of different prime factors contained in τ.

We shall show that the sum (11) vanishes. We observe that if τ be expressed as in (9),

$$f(\tau) = f(\pi_1^{e_1}) f(\pi_2^{e_2}) \cdots f(\pi_r^{e_r}).$$

Also if the highest power of a prime π contained in λ/σ be π^h,

$$\sum_{e=1}^{h} \frac{f(\pi^e)}{\pi^{2e-1}} = \frac{\pi - 1}{\pi} + \frac{\pi^2 - \pi}{\pi^3} + \cdots + \frac{\pi^{h-1} - \pi^{h-2}}{\pi^{2h-3}} + \frac{\pi^h}{\pi^{2h-1}} = 1.$$

Hence if

$$\lambda/\sigma = \pi_1^{h_1} \pi_2^{h_2} \cdots \pi_s^{h_s},$$

then

$$\sum_{e_i=1}^{h_i} \frac{f(\pi_1^{e_1} \pi_2^{e_2} \cdots \pi_r^{e_r})}{\pi_1^{2e_1-1} \pi_2^{2e_2-1} \cdots \pi_r^{2e_r-1}} = 1.$$

Hence the sum (11) may be written

$$\sum_{r=0}^{s} (-1)^r \binom{s}{r} = 0.$$

Consequently equation (10) is true and equations (5) therefore completely determine the quantities m_i^j.

Determination of the numbers m_i^j for a special type of field.

4. We shall now obtain exact expressions for the numbers m_i^j for a field of order q^{2t}, provided there exists an exponent t_1, where $t = st_1$, such that $q^{t_1} \equiv -1$, mod λ. We have in this case by a result established in the author's other paper*

$$(1) \qquad \sum_{i,\, j} m_i^j \alpha^{aj+bi} = (-1)^{s-1} q^t,$$

where α is a primitive λth root of unity, a, b are any integers such that $a \not\equiv 0$, $b \not\equiv 0$, $a + b \not\equiv 0$, mod λ, and i, j range independently over the residues $0, 1, 2, \cdots, \lambda - 1$.

For a field of this sort, if q is odd, ν must be even, and hence $\epsilon \equiv$ ind $(-1) \equiv 0$, mod λ. We therefore find from equations (1) and (2), § 3, that the value of the left-hand side of equation (1) is -1 in case exactly one of the three congruences

---

* L. c., p. 177.

$$a \equiv 0, \qquad b \equiv 0, \qquad a + b \equiv 0, \qquad \text{mod } \lambda,$$

is satisfied, and $q^{2t} - 2$ in case all three are satisfied.

If, as previously, we assume that $dv(\lambda, a, b) = 1$, we may write

$$\sum_c M_{a,b,c}\alpha^{kc} = (-1)^{s-1}q^t, \ -1, \ q^{2t} - 2, \tag{2}$$

according as none of the congruences

$$ka \equiv 0, \qquad kb \equiv 0, \qquad k(a + b) \equiv 0, \qquad \text{mod } \lambda, \tag{3}$$

is satisfied, one of them is satisfied, or all three are satisfied, where $M_{a,b,c}$ has the meaning defined in § 3, and $c = 0, 1, 2, \cdots, \lambda - 1$.

We write

$$dv(\lambda, a) = a', \qquad dv(\lambda, b) = b', \qquad dv(\lambda, a + b) = d'. \tag{4}$$

If we multiply each of the equations (2) by α^{-kc}, where c is fixed, and then form the sum for $k = 0, 1, 2, \cdots, \lambda - 1$, we obtain

$$M_{a,b,c} = \frac{1}{\lambda}\left[q^{2t} - 2 - \sum_k \alpha^{-kc} + (-1)^{s-1}q^t\sum_k \alpha^{-kc}\right], \tag{5}$$

where in the first of the two sums on the right k assumes the $a' + b' + d' - 3$ values for which exactly one of the congruences (3) is satisfied, and in the second sum the $\lambda - a' - b' - d' + 2$ values for which none of them are satisfied.

The sum of the expressions α^{-kc} for the $a' - 1$ values of k other than 0 for which the first of the congruences (3) is satisfied is $a' - 1$ or -1 according as c is or is not divisible by a', and similarly for the other two sets of the same sort. The sum of all the $\lambda - 1$ expressions α^{-kc} $(k = 1, 2, \cdots, \lambda - 1)$ is $\lambda - 1$ or -1 according as $c \equiv 0, \not\equiv 0$, mod λ. Hence the values of $M_{a,b,c}$ in the various cases are:

$$(5a) \quad M_{a,b,0} = \frac{1}{\lambda}[q^{2t} + (\lambda + 2 - a' - b' - d')(-1)^{s-1}q^t \\ - (a' + b' + d') + 1];$$

$$(5b) \quad M_{a,b,c} = \frac{1}{\lambda}[q^{2t} + (2 - a' - b' - d')(-1)^{s-1}q^t - (a' + b' + d') + 1],$$

for $c \not\equiv 0$, mod λ, $c \equiv 0$, mod a', b', d';

$$(5c) \quad M_{a,b,c} = \frac{1}{\lambda}[q^{2t} + (2 - a' - b')(-1)^{s-1}q^t - (a' + b') + 1],$$

for $c \not\equiv 0$, mod d', $c \equiv 0$, mod a', b';

$$(5d) \quad M_{a,b,c} = \frac{1}{\lambda}[q^{2t} + (2 - a')(-1)^{s-1}q^t - a' + 1],$$

for $c \not\equiv 0$, mod b', d', $c \equiv 0$, mod a';

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} + 2(-1)^{s-1}q^t + 1], \tag{5e}$$

for $c \not\equiv 0$, mod a', b', d'. Any other case is essentially equivalent to one of these.

We first suppose that λ is prime. In this case a', b', d' all have the value 1, or one has the value λ and the other two the value 1, according as none of the congruences

$$a \equiv 0, \qquad b \equiv 0, \qquad a + b \equiv 0, \quad \text{mod } \lambda, \tag{6}$$

is satisfied, or one of them is satisfied. Hence if $c \equiv 0$, mod λ, we have in these two cases

$$M_{a,b,0} = \frac{1}{\lambda}[q^{2t} + (\lambda - 1)(-1)^{s-1}q^t - 2], \tag{7}$$

$$M_{a,b,0} = \frac{1}{\lambda}[q^{2t} - \lambda - 1], \tag{7'}$$

respectively, whereas if $c \not\equiv 0$, mod λ, we have correspondingly

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} - (-1)^{s-1}q^t - 2], \tag{8}$$

$$M_{a,b,c} = \frac{1}{\lambda}[q^{2t} - 1]. \tag{8'}$$

There are for λ prime $\lambda^2 + \lambda$ equations of the type (5), § 3, and a particular $m_{i_0}^{j_0}$ appears in $\lambda + 1$ of these, i. e., the equations E_1 of § 3. For any other m_i^j the value of σ [see (6), § 3] is 1, so that it appears exactly once in the equations E_1. The sum of the left-hand members of these equations E_1 is therefore [by use of equations (2), § 3] equal to

$$\lambda m_{i_0}^{j_0} + q^{2t} - 2. \tag{9}$$

For i_0, $j_0 \equiv 0$, 0, mod λ, three of the right-hand members of the $\lambda + 1$ equations E_1 have the value given by (7′) and the rest the value given by (7). If exactly one of the three congruences

$$i_0 \equiv 0, \qquad j_0 \equiv 0, \qquad i_0 \equiv j_0, \quad \text{mod } \lambda,$$

is satisfied, one of the right-hand members has the value given by (7′), two the value given by (8′), and the rest the value given by (8). If none of those congruences are satisfied, one has the value given by (7), three the value given by (8′), and the rest the value given by (8).

If, therefore, we add these values and equate the results to (9), we obtain in the three cases

$$
\begin{aligned}
&m_0{}^0 = \frac{1}{\lambda^2}[q^{2t} + (\lambda - 1)(\lambda - 2)(-1)^{s-1}q^t - 3\lambda + 1],\\
(10)\qquad &m_i{}^0 = m_0{}^i = m_{-i}^{-i} = \frac{1}{\lambda^2}[q^{2t} - (\lambda - 2)(-1)^{s-1}q^t - \lambda + 1],\\
&m_i{}^j = \frac{1}{\lambda^2}[q^{2t} + 2(-1)^{s-1}q^t + 1],
\end{aligned}
$$

where $i \not\equiv 0$, $j \not\equiv 0$, $i \not\equiv j$, mod λ.

Dickson* and Hurwitz* have established certain limits for the numbers $m_i{}^j$ for λ prime, and for a field of order q. Corresponding limits may be shown to hold for any field by their methods, provided λ is prime. The value of $m_0{}^0$ given above coincides with the upper or lower limit which they have obtained according as s is odd or even.

We shall show that equations (10) are also true if λ is composite. In view of Theorem 1, we may do this by showing that the values given by (10) satisfy equations (5), § 3. A sum $M_{a,b,0}$ having the value given by (5a) contains $m_0{}^0$, $a' - 1$ numbers $m_0{}^i$, $b' - 1$ numbers $m_i{}^0$, $d' - 1$ numbers $m_i{}^i$, and $\lambda - a' - b' - d' + 2$ numbers $m_i{}^j$, where $i \not\equiv 0$, $j \not\equiv 0$, $i \not\equiv j$, mod λ. When the values given by (10) are substituted, the result is found to coincide with the known value given by (5a). We find the same to be true in the other four cases, distinguished according to the divisibility of c by a', b', d'.

We therefore have

Theorem 2. *If* $q^{t_1} \equiv -1$, *mod* λ, *and* $t = st_1$, *the values of the numbers* $m_i{}^j$ *for a field of order* q^{2t} *are given by equations* (10).

A relation between the numbers $m_i{}^j$ for different fields.

5. We suppose now that $q^t \equiv 1$, mod λ, and denote by ${}_sm_i{}^j$ and $m_i{}^j$ the numbers of solutions of the congruences for the fields of order q^{st} and q^t respectively. We suppose also that the primitive roots g_s and g in these two fields are so chosen that $g_s{}^{\nu_s} \equiv g^\nu$, where

$$
\nu_s = \frac{q^{st} - 1}{\lambda}, \qquad \nu = \frac{q^t - 1}{\lambda}.
$$

In the author's previous paper† it was shown that, if this condition is satisfied, the cyclotomic functions for the two fields are connected by the relation

$$
(1)\qquad \sum_{i,j} {}_sm_i{}^j\alpha^{aj+bi} = (-1)^{s-1}\{\sum_{i,j} m_i{}^j\alpha^{aj+bi}\}^s,
$$

---

* L. c.

† L. c., p. 176.

where, as above, α denotes a primitive λth root of unity, a, b are any two integers such that $a \not\equiv 0$, $b \not\equiv 0$, $a + b \not\equiv 0$, mod λ, and i, j range independently over the residues $0, 1, 2, \cdots, \lambda - 1$.

The relation (1) also holds if one of the congruences $a \equiv 0$, $b \equiv 0$, $a + b \equiv 0$, mod λ, is satisfied. For in that case the value of each of the functions is -1 unless q and ν (or ν_s) are both odd, $a \equiv 0$, mod λ, and b is odd, in which case it is $+1$.* But if q and ν are both odd, then ν_s is odd or even with s, and hence the value of the function for the field of order q^{st} is $(-1)^{s-1}$.

If we replace α by α^k and suppose that $dv(\lambda, a, b) = 1$, we may write equation (1) in the form

$$(2) \qquad \sum_{c} {}_sM_{a,b,c}\alpha^{kc} = (-1)^{s-1}\sum_{c} S_{a,b,c}\alpha^{kc},$$

where k has any residue, mod λ, except 0, ${}_sM_{a,b,c}$ denotes the sum of the numbers ${}_sm_i^j$ for which

$$aj + bi \equiv c, \qquad \text{mod } \lambda,$$

and $S_{a,b,c}$ denotes the sum of all products of the form

$$(3) \qquad m_{i_1}^{j_1} m_{i_2}^{j_2} \cdots m_{i_s}^{j_s},$$

where the indices assume all residues as values, mod λ, for which

$$a(j_1 + j_2 + \cdots + j_s) + b(i_1 + i_2 + \cdots + i_s) \equiv c, \qquad \text{mod } \lambda.$$

For $k \equiv 0$, mod λ, we may write, in view of equations (2), § 3,

$$(2') \qquad \sum_{c} {}_sM_{a,b,c} = q^{st} - 2 + (-1)^s(q^t - 2)^s + (-1)^{s-1}\sum_{c} S_{a,b,c}.$$

From the equations (2), (2′) we obtain

$${}_sM_{a,b,c} = \frac{1}{\lambda}\left[q^{st} - 2 + (-1)^s(q^t - 2)^s\right] + (-1)^{s-1}S_{a,b,c}.$$

We observe that equations (5), § 3, will all be satisfied provided the numbers ${}_sm_i^j$ have the values

$$(4) \qquad {}_sm_i^j = \frac{1}{\lambda^2}\left[q^{st} - 2 + (-1)^s(q^t - 2)^s\right] + (-1)^{s-1}s_i^j,$$

where s_i^j denotes the sum of all the products of the form (3) for which

$$i_1 + i_2 + \cdots + i_s \equiv i, \qquad j_1 + j_2 + \cdots + j_s \equiv j, \qquad \text{mod } \lambda.$$

In view of Theorem 1, we have therefore

Theorem 3. *If* $q^t \equiv 1$, *mod* λ, *and if the primitive roots* g_s *and* g *in the fields of order* q^{st} *and* q^t *be so chosen that* $g_s^{\nu_s} \equiv g^{\nu}$, *then the numbers* ${}_sm_i^j$ *for the field of order* q^{st} *may be expressed in terms of the numbers* m_i^j *for the field of order* q^t *by means of equations* (4).

UNIVERSITY OF PENNSYLVANIA,
PHILADELPHIA, PA.

---

* This may be shown by means of equations (1) and (2), § 3, of the present paper.